CLAIMS

1. Apparatus (200) for mediating in management orders between a plurality of origin managers (101,102,10x) and a plurality of managed devices -(301,302,30x) in a telecommunications system, said management orders intended to execute management operations over said managed devices; CHARACTERIZED in that it comprises:
   - a Communication Receiver Component (201), arranged to receive a management order from an origin manager,
   - a Management Verifier Component (202), arranged to determine whether a received management order is an allowed management order by checking whether said management order fits an access attribute comprised in a management access template selected from:

     a first management access template (501) in relationship with an identifier of said origin manager,

     a second management access template (503) in relationship with an identifier of a managed data object affected by said management order, and

     a third management access template (504) in relationship with an identifier of a managed device affected by said management order,

   and
   - a Communication Sender Component (203), arranged to send an allowed management order to a managed device.

2. The apparatus of claim 1, wherein said first management access template comprises at least one access attribute selected from:
   - an identifier of an allowed management operation,
   - an identifier of an allowed managed data object,
   - a pattern structure of said managed data object,
   - an identifier of an allowed managed device,

- an identifier of an allowed management operation over an allowed managed device,
- an identifier of an allowed management operation over an allowed managed data object.

3. The apparatus of claim 1, wherein said second management access template comprises at least one access attribute selected from:
   - a pattern structure of said managed data object,
   - an identifier of an allowed management operation,
   - an identifier of a managed device holding said managed data object,
   - an identifier of an allowed origin manager,
   - an identifier of an allowed management operation from an allowed origin manager,
   - an identifier of an allowed management operation over a holding managed device.

4. The apparatus of claim 1, wherein said third management access template comprises at least one access attribute selected from:
   - an identifier of an allowed management operation,
   - an identifier of a managed data object held on said managed device,
   - an identifier of an allowed origin manager,
   - an identifier of an allowed management operation from an allowed origin manager,
   - an identifier of an allowed management operation over a held managed data object.

5. The apparatus of claim 1, wherein said Management Verifier Component is arranged to determine, from the identifier of a management operation, at least one identifier selected from:

- an identifier of a managed data object affected by said operation, and
- an identifier of a managed device, affected by said operation.

6. The apparatus of claim 1, wherein said Management Verifier Component is arranged to select a management access template, among said first second and third management templates, according to an identifier received in a management order.

7. The apparatus of claim 6, wherein said Management Verifier Component is arranged to select a management access template, among said first second and third management templates, according to an access attribute comprised in another selected management access template.

8. The apparatus of claims 6 or 7, wherein the identifier (ORID) of an origin manager (101) comprises at least one identifier among:

- an identifier of a management server (101-2) sending a management order,
- an identifier of a user (101-1) operating said management server,

and wherein said Management Verifier Component is arranged to select said first management access template according to said at least one identifier.

9. The apparatus of claims 6 or 7, wherein the identifier (ORID) of an origin manager (101) comprises at least one identifier among:

- an identifier of a management server (101-2) sending a management order,
- an identifier of a user (101-1) operating said management server,

and wherein said Management Verifier Component is arranged to authenticate said at least one identifier.

10. The apparatus of claims 6 or 7, wherein said Management Verifier Component is arranged to determine a management role associated to at least one identifier selected from:

- an identifier of a management server (101-2) sending a management order,
- an identifier of a user (101-1) operating said management server.

11. The apparatus of claim 10, wherein said Management Verifier Component is further arranged to select at least one management access template (502) in relationship with said role.

12. The apparatus of claim 10, wherein at least one management access template among said second or third management templates comprises an identifier (ROm) of at least one role as an access attribute, and wherein said Management Verifier Component is further arranged to check whether said management order fits with said role.

13. The apparatus of any of claims 1 to 12, wherein said Management Verifier Component is arranged to determine whether a managed data object affected by an allowed management order is an access attribute in a management access template, further comprising an Management Execution Component, arranged to execute a management operation over said access attribute.

14. The apparatus of any of claims 1 to 12, wherein said Communication Receiver Component is further arranged to receive an access request from an origin manager,

wherein said Management Verifier Component is further arranged to determine said first management access template, and wherein said Communication Sender Component is further arranged to send an access response to said origin manager that comprises an access attribute of said management access template.

15. In a telecommunications system, a method for mediating in the management of a plurality of devices (301,302,30x) from a plurality of origin managers (101,102,10x); wherein the management of a managed device comprises the steps of:

- receiving a management order from an origin manager in said managed device, and
- executing a management operation requested by said management order in said managed device;

CHARACTERIZED in that, for mediating in said management order, the step of receiving further comprises the steps of:

- receiving a management order in a centralized management mediator (200),
- checking in said centralized management mediator whether said management order fits an access attribute comprised in a management access template selected from:

  a first management access template (501) in relationship with an identifier of said origin manager,

  a second management access template (503) in relationship with an identifier of a managed data object affected by said management order, and

  a third management access (504) template in relationship with an identifier of a managed device affected by said management order, to determine whether a received management order is an allowed management order, and

- granting said management order to be sent to a managed device if it is an allowed management order.

16. The method of claim 15, wherein the step of checking said management order further comprises the step of determining, from the identifier of a management operation, at least one identifier selected from:

- an identifier of a managed data object affected by said operation, and
- an identifier of a managed device, affected by said operation.

17. The method of claim 15, wherein the step of checking said management order further comprises the step of selecting a management access template, among said first second and third management templates, according to an identifier received in a management order.

18. The method of claim 17, wherein the step of checking said management order further comprises the step of selecting a management access template, among said first second and third management templates, according to an access attribute comprised in another selected management access template.

19. The method of claims 17 or 18, wherein the identifier (ORID) of an origin manager (101) comprises at least one identifier among:

- an identifier of a management server (101-2) sending a management order,
- an identifier of a user (101-1) operating said management server,

and wherein the step of selecting a management access template comprises the step of selecting said first management access template according to said at least one identifier.

20. The method of claims 17 or 18, wherein the identifier (ORID) of an origin manager (101) comprises at least one identifier among:
    - an identifier of a management server (101-2) sending a management order,
    - an identifier of a user (101-1) operating said management server,

    and wherein the step of checking said management order further comprises the step of authenticating said at least one identifier.

21. The method of claims 17 or 18, wherein the step of checking said management order further comprises the step of determining a management role associated to at least one identifier selected from:
    - an identifier of a management server (101-2) sending a management order,
    - an identifier of a user (101-1) operating said management server.

22. The method of claim 21, wherein the step of checking said management order further comprises the step of selecting a management access template (502) in relationship with said role.

23. The method of claim 21, wherein at least one management access template among said second or third management templates comprises an identifier (ROm) of at least one role as an access attribute, and wherein the step of checking said management order further comprises the step of checking whether said management order fits with said role.

24. The method of any of claims 15 to 23, wherein the step of checking said management order further comprises the step of:
    - checking whether a managed data object affected by an allowed management order is an access attribute in a management access template,

    and wherein the step of granting said management order comprises the step of:
    - executing a management operation over said access attribute.

25. The method of any of claims 15 to 23, further comprising the steps of:
    - receiving an access request from an origin manager,
    - determining said first management access template, and
    - sending an access response to said origin manager that comprises an access attribute of said management access template.

26. A computer program for mediating from a computer-based apparatus (200) in management orders between a plurality of origin managers (101,102,10x) and a plurality of managed devices (301,302,30x) in a telecommunications system, said management orders intended to execute management operations over said managed devices; CHARACTERIZED in that it comprises:
    - a computer-readable program code for causing said computer-based apparatus to process the reception of a management order from an origin manager,
    - a computer-readable program code for causing said computer-based apparatus to determine whether a received management order is an allowed management order by checking whether said management order fits

an access attribute comprised in a management access template selected from:

a first management access template (501) in relationship with an identifier of said origin manager,

a second management access template (503) in relationship with an identifier of a managed data object affected by said management order, and

a third management access template (504) in relationship with an identifier of a managed device affected by said management order,

and

- a computer-readable program code for causing said computer-based apparatus to send an allowed management order to a managed device.

27. The computer program of claim 26, further comprising a computer-readable program code for causing said computer-based apparatus to determine, from the identifier of a management operation, at least one identifier selected from:

- an identifier of a managed data object affected by said operation, and
- an identifier of a managed device, affected by said operation.

28. The computer program of claim 26, further comprising a computer-readable program code for causing said computer-based apparatus to select a management access template, among said first second and third management templates, according to an identifier received in a management order.

29. The computer program of claim 28, further comprising a computer-readable program code for causing said

computer-based apparatus to select a management access template, among said first second and third management templates, according to an access attribute comprised in another selected management access template.

30. The computer program of claims 28 or 29, wherein the identifier (ORID) of an origin manager (101) comprises at least one identifier among:

- an identifier of a management server (101-2) sending a management order,
- an identifier of a user (101-1) operating said management server,

further comprising a computer-readable program code for causing said computer-based apparatus to select said first management access template according to said at least one identifier.

31. The computer program of claims 28 or 29, wherein the identifier (ORID) of an origin manager (101) comprises at least one identifier among:

- an identifier of a management server (101-2) sending a management order,
- an identifier of a user (101-1) operating said management server,

further comprising a computer-readable program code for causing said computer-based apparatus to authenticate said at least one identifier.

32. The computer program of claims 28 or 29, further comprising a computer-readable program code for causing said computer-based apparatus to determine a management role associated to at least one identifier selected from:

- an identifier of a management server (101-2) sending a management order,

- an identifier of a user (101-1) operating said management server.

33. The computer program of claim 32, further comprising a computer-readable program code for causing said computer-based apparatus to select at least one management access template (502) in relationship with said role.

34. The computer program of claim 32, wherein at least one management access template among said second or third management templates comprises an identifier (ROm) of at least one role as an access attribute, further comprising a computer-readable program code for causing said computer-based apparatus to check whether said management order fits with said role.

35. The computer program of any of claims 26 to 34, further comprising a computer-readable program code for causing said computer-based apparatus to determine whether a managed data object affected by an allowed management order is an access attribute in a management access template, and a computer-readable program code for causing said computer-based apparatus to execute a management operation over said access attribute.

36. The computer program of any of claims 26 to 34, further comprising:
   - a computer-readable program code for causing said computer-based apparatus to process the reception of an access request from an origin manager,
   - a computer-readable program code for causing said computer-based apparatus to determine said first management access template, and
   - a computer-readable program code for causing said computer-based apparatus to send an access response

to said origin manager that comprises an access attribute of said management access template.